

IN THE CLAIMS:

1. A method for communicating securely over an insecure communication channel between a pair of correspondents who perform shared key cryptographic operations by implementing respective ones of a pair of complimentary mathematical operations utilizing a shared key, said method comprising the steps of:

assembling a data string including information to be transferred from a sending correspondent to a receiving correspondent;

performing a complimentary mathematical operation using points on an elliptic curve defined over a finite field and represented in projective coordinates, and wherein the addition of points on the elliptic curve is defined in projective coordinates; and

forwarding the defined group of points over a communication channel to the receiving correspondent and performing the other of the corresponding mathematical cryptographic operations to decrypt the data.

2. A method of encrypting and decrypting a message bit string in an information processing system in accordance with claim 1 where the elliptic curve points in projective coordinates are represented using three coordinates, (X, Y, Z) , wherein X , Y and Z are elements of $F(p)$ represented in N -bit strings, and which includes a step where extra message bits are embedded in the Z coordinate in addition to the message data bits that are embedded in the X coordinate,

3. A method of encrypting and decrypting a message bit string in an information processing system in accordance with claim 2 comprising the steps of:

embedding a message bit string into the X and Z coordinates of an elliptic curve point which is designated as the message point, $(X_m Y_m Z_m)$;

providing a shared key k and a base point $(X_b Y_b Z_b)$ and computing the scalar multiplication $(X_{bk} Y_{bk} Z_{bk}) = k (X_b Y_b Z_b)$;

computing a cipher point $(X_c Y_c Z_c)$ using $(X_c Y_c Z_c) = (X_m Y_m Z_m) + k(X_b Y_b Z_b)$;

sending appropriate bits of the X -coordinate, X_c and the Z -coordinate Z_c of the cipher point $(X_c Y_c Z_c)$ to a receiving party;

using the shared key k and the base point $(X_b Y_b Z_b)$ computing the scalar multiplication $(X_{bk} Y_{bk} Z_{bk}) = k (X_b Y_b Z_b)$;
 computing the message point $(X_m Y_m Z_m)$ using $(X_m Y_m Z_m) = (X_c Y_c Z_c) + (-k (X_b Y_b Z_b))$;
 recovering the message bit string from X_m and Z_m .

4 A method for encrypting and decrypting a message bit string in an information processing system according to claim 3 in which the message bit string is divided into strings of length of M -bit where $(2N-L) > M > (N-L)$.

5 A method for encrypting and decrypting a message bit string in an information processing system according to claim 4 in which a M -bit message string is further divided into two strings $m_1 m_2$, where the length of string m_1 must be no more than $(N-L)$ bits, while the length of string m_2 must be no more than $(N-1)$ bits.

6. A method for encrypting and decrypting a message bit string in an information processing system according to claim 5 which includes the steps of:

assigning the value of the bit string of m_2 to Z_m using the following procedure:

- i. assign the value of the bit string m_2 to R_m ,
- ii. using Legendre test to determine if R_m has a square root,
- iii. if R_m has a square root set $Z_m = R_m$ otherwise set $Z_m = gR_m$ where g is any non-quadratic value in the underlying finite field,

and compute a Z_m^2 and bZ_m^3

assign the value of the bit string of m_1 to X_m

compute $T = X_m^3 + (aZ_m^2) X_m + (bZ_m^3)$;

using Legendre test to see if T has a square root;

if T has a square root assign one of the roots to Y , if not continue incrementing X_m and repeating the computation of T until T has a square root.

7. A method for transferring data over a communication channel according to claim 6 in which a second projective coordinate is used by the sending correspondent and to the receiving correspondent to eliminate the inversion or division during each addition and doubling operation of the scalar multiplication.

8. An encryption and decryption system in accordance with claim 7 and which is implemented either as a pure hardware unit, or as a program stored on a computer readable storage device and executed on a digital computer, or a combination of both.

9. A method for transferring data over a communication channel between a pair of correspondents who perform public key cryptographic operations by implementing respective ones of a pair of complimentary mathematical operations utilizing a public key and a private key of one of the correspondents, said method comprising the steps of:

assembling a data string including information to be transferred from a sending correspondent to a receiving correspondent;

performing a complimentary mathematical operation using a group of points on an elliptic curve defined over a finite field and represented in projective coordinates, and wherein the group of points on the elliptic curve are defined over addition in projective coordinates; and

forwarding the defined group of points over a communication channel to the receiving correspondent and performing the other of the corresponding mathematical operations of the public key and the private key cryptographic operation to decrypt the data.

10. A method of encrypting and decrypting a message bit string in an information processing system in accordance with claim 9 where the elliptic curve points in projective coordinates are represented using three coordinates, (X,Y,Z) , wherein X , Y and Z are elements of $F(p)$ represented in N -bit strings, and which includes a step of embedding extra message bits in the Z coordinate in addition to the message data bits that are embedded in the X coordinate.

11. A method of encrypting and decrypting a message bit string in an information processing system in accordance with claim 10 comprising the steps of:

embedding a message bit string into the X and Z coordinates of an elliptic curve point which is designated as the message point, $(X_m Y_m Z_m)$ by the sending correspondent;

using the private key of the sending correspondent, k_{SPr} , and the public key of the receiving correspondent, $k_{RPt}(X_b Y_b Z_b)$, to compute the scalar multiplication $(X_{bk} Y_{bk} Z_{bk}) = k_{SPr} (k_{RPt} (X_b Y_b Z_b))$;

computing a cipher point $(X_c Y_c Z_c)$ using $(X_c Y_c Z_c) = (X_m Y_m Z_m) + (X_{bk} Y_{bk} Z_{bk})$;

sending appropriate bits of the X-coordinate, X_c and the Z-coordinate Z_c of the cipher point $(X_c Y_c Z_c)$ to the receiving correspondent;

using the private key of the receiving correspondent, k_{RPt} , and the public key of the sending correspondent, $k_{SPr}(X_b Y_b Z_b)$, to compute the scalar multiplication $(X_{bk} Y_{bk} Z_{bk}) = k_{RPt} (k_{SPr} (X_b Y_b Z_b))$;

computing the message point $(X_m Y_m Z_m)$ using $(X_m Y_m Z_m) = (X_c Y_c Z_c) - (X_{bk} Y_{bk} Z_{bk})$;

recovering the message bit string from X_m and Z_m .

12. A method for encrypting and decrypting a message bit string in an information processing system according to claim 11 in which the message bit string is divided into strings of length of M-bit where $(2N-L) > M > (N-L)$.

13. A method for encrypting and decrypting a message bit string in an information processing system according to claim 12 in which a M-bit message string is further divided into two strings $m_1 m_2$, where the length of string m_1 must be no more than $(N-L)$ bits, while the length of string m_2 must be no more than $(N-1)$ bits.

14. A method for encrypting and decrypting a message bit string in an information processing system according to claim 13 which includes the steps of:

assigning the value of the bit string of m_2 to Z_m using the following procedure:

- iv. assign the value of the bit string m_2 to R_m ,
- v. using Legendre test to determine if R_m has a square root,

- vi. if R_m has a square root set $Z_m = R_m$ otherwise set $Z_m = gR_m$ where g is any non-quadratic value in the underlying finite field,

and compute aZ_m^2 and bZ_m^3

assign the value of the bit string of m_1 to X_m

compute $T = X_m^3 + (aZ_m^2) X_m + (bZ_m^3)$;

using Legendre test to see if T has a square root;

if T has a square root assign one of the roots to Y , if not continue incrementing X_m and repeating the computation of T until T has a square root.

15. A method for transferring data over a communication channel according to claim 14 in which a second projective coordinate is used by the sending correspondent and to the receiving correspondent to eliminate the inversion or division during each addition and doubling operation of the scalar multiplication.

16. An encryption and decryption system in accordance with claim 15 and which is implemented as a pure hardware unit, or as a program stored on a computer readable storage device and executed on a digital computer.

17. In a method for communicating securely over an insecure communication channel using elliptic curve cryptography, the improvement comprising applying projective coordinates in two stages and wherein a projective coordinate in a first of said two stages is used to embed extra message data bits in the Z -coordinate and wherein a projection coordinate in a second of said two stages is used to remove a division operation at each iteration and for randomizing the computation in order to provide a counter measure against differential power analysis.

18. A method of digital signatures generation and verification using points on an elliptic curve defined over a finite field and represented in projective coordinates, and wherein the addition of points on the elliptic curve is defined in projective coordinates.

19. A method of digital signature generation and verification in accordance with claim 18 which involves mathematical operations that includes steps of elliptic curve scalar multiplication(s) using point additions defined in projective coordinates.
20. A method of digital signature generation and verification in accordance with claim 19 where both the X and Z coordinate of the computed elliptic curve point(s) are used in the signature generation and verification steps.
21. A method of digital signature generation and verification in accordance with claim 20 in which a second projective coordinate is used by the signing correspondent and to the verifying correspondent to eliminate the inversion or division during each addition and doubling operation of the corresponding scalar multiplication, and for randomizing the computation in order to provide a counter measure against differential power analysis.
22. A digital signature generation and verification system in accordance with claim 21 and which is implemented either as a pure hardware unit, or as a program stored on a computer readable storage device and executed on a digital computer, or a combination of both.